AO 106 (REV 4/10) Affidavit for Search Warrant — AUSA Sean K. Driscoll, (312) 469-6151

FILED

OCT 26 2018

MAGISTRATE JUDGE SUSAN E. COX
UNITED STATES DISTRICT COURT

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

**UNDER SEAL**

In the Matter of the Search of:

The Google account executivedata58@gmail.com, further described in Attachment A

Case Number:

18M678

# APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Timothy J. Malak, a Special Agent of the Federal Bureau of Investigation (FBI), request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

**See Attachment A**

located in the Northern District of California, there is now concealed:

**See Attachment A**

The basis for the search under Fed. R. Crim. P. 41(c) is evidence, instrumentalities, and fruits.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| Title 18, United States Code, Section 1028 | Identity theft |
| Title 18, United States Code, Section 1028A | Aggravated identity theft |
| Title 18, United States Code, Section 1343 | Wire fraud |

The application is based on these facts:

**See Attached Affidavit,**

Continued on the attached sheet.

*Applicant's Signature*

TIMOTHY J. MALAK, Special Agent, FBI
*Printed name and title*

Sworn to before me and signed in my presence.

Date: October 26, 2018

*Judge's signature*

City and State: Chicago, Illinois

SUSAN E. COX, U.S. Magistrate Judge
*Printed name and title*

1

UNITED STATES DISTRICT COURT )
)
NORTHERN DISTRICT OF ILLINOIS )

**AFFIDAVIT**

I, Timothy J. Malak, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately July 2017.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to computer crimes. I have participated in the execution of multiple federal search warrants.

3. This affidavit is made in support of an application for a warrant to search, pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with certain account(s) that are stored at the premises owned, maintained, controlled, or operated by Google, a free web-based electronic mail service provider located at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The account to be searched is executivedata58@gmail.com (hereinafter, "**Subject Account 18**"), which is further described in the following paragraphs and in Part II of Attachment A. As set forth below, there is probable cause to believe that in the account, described in Part II of Attachment A, in the possession of Google, there exists evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 1028, 1028A, and 1343 (hereinafter the "**Subject Offenses**").

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence, instrumentalities, and fruits of violations of the **Subject Offenses** are located in **Subject Account 18**.

## I. BACKGROUND INFORMATION

### A. Google

5. Based on my training and experience and information available from Google's website (google.com), I have learned the following information about Google and Gmail:

a. Google offers a collection of Internet-based services, including e-mail and online data storage, which is owned and controlled by Google. The services are available at no cost to Internet users, though there are certain options, such as additional online data storage, that users may elect to pay money to receive. Subscribers obtain an account by registering on the Internet with Google and providing Google with basic information, including name, gender, zip code, and other personal/biographical information. Subscribers are given a Google account which ends in "@gmail.com" which is utilized to access these online services.

b. Google maintains electronic records pertaining to the individuals and entities who maintain Google online subscriber accounts. These records often include account access information, e-mail transaction information, account application information, and in some circumstances billing and payment information.

c. Any e-mail that is sent to a Google online account subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by Google. If the message is not deleted by the subscriber, the account is below the maximum storage limit, and the subscriber accesses the account periodically, that message can remain on Google's servers indefinitely.

d. When a subscriber sends an e-mail, it is initiated by the user, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google online account users have the option of saving a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail may remain on the system indefinitely.

e. Google online account subscribers can store files, including but not limited to e-mails, documents, and image files, on servers maintained and/or owned by Google. The online data storage service is known as "Google Drive."

f. Google online account subscribers can also utilize a feature known as "History" that allows a user to track various historical account activity, including past Google Internet searches performed, information regarding devices

which have been used to login to the Google online account, and physical location information regarding from where the Google online account was accessed.

g. Google keeps records that can reveal accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites.

6. Therefore, the computers of Google are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Google, such as account access information, transaction information, and account application. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Google, to protect the rights of the subjects of the investigation and to effectively pursue this investigation, authority is sought to allow Google to make a digital copy of the entire contents of the information subject to seizure specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A.

## II. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH THE SUBJECT ACCOUNT

7. The FBI is investigating spearphishing emails sent to several U.S. businesses, which sought W-2 forms (including social security numbers) for the businesses' employees. The emails purported to be from high-ranking employees of

the businesses in the United States, but were in fact all sent from unknown and unauthorized external email addresses. Several of the spearphishing emails were successful and W-2 forms (including social security numbers) for numerous employees were fraudulently obtained as a result of these emails. In addition to phishing for employee W-2 forms, fraudulent requests for wire transfers occurred. At least one of the fraudulent wire requests was sent by **Subject Account 18** to Company E, a search of which may reveal the identity of the individual who sent the spearphishing emails.

***Spearphishing Emails Sent to Company A in 2017***

8. According to email records provided by Company A to the FBI, on or about February 2, 2017, Employee A of Company A received an email at his/her official Company A email address. The sender's name for this email purported to be Individual A, the Chief Financial Officer of Company A, but the actual email address was MD.BIZ@AOL.COM (which is Subject Account 1). The email requested "the 2016 W-2 (PDF) of every member of staff for a quick financial review."

9. According to email records provided by Company A to the FBI, on the same date Employee A responded to the email from Subject Account 1, and attached a PDF file with approximately 850 W-2 forms for Company A's employees. According to Company A, Subject Account 1 was not authorized to request or receive this information.

10. According to Company A, several hundred employees from Company A who reside in the Northern District of Illinois had their W-2 information lost due to the spearphishing email attack. Additionally, the email server for Company A is comprised of computer systems physically located in the Northern District of Illinois, and the employee records that Employee A mistakenly sent are stored on Company A's computer servers in the Northern District of Illinois.

***Spearphishing Emails Sent to Company B in 2017***

11. According to email records provided by Company B to the FBI, on or about February 7, 2017, Employee B of Company B received an email at his/her official Company B email address. The sender's name for this email purported to be Individual B, who is the Chief Financial Officer of Company B, but the actual email address was MD.BIZ@AOL.COM (Subject Account 1, which is the same account that emailed Company A). The email had the same wording as the spearphishing email sent to Company A, and read: "Kindly send me the 2016 W-2 (PDF) of every member of staff for a quick financial review."

12. According to Company B, Employee B did not provide W2 information in response to the email from Subject Account 1 sent in 2017.

***Spearphishing Email Sent to Company B in 2018***

13. According to email records provided by Company B to the FBI, on or about February 16, 2018, Employee B of Company B received an email at his/her official Company B email address. The sender's name for this email purported to be

Individual B, the Chief Financial Officer of Company B, but the actual email address was CEO_PORT@COMCAST.NET (which is Subject Account 2). The email, which was nearly identical to the emails sent from Subject Account 1 to Company A and Company B one year prior, read: "Kindly send me the individual 2017 W-2 (PDF) of our company staff for a quick review."

14. According to email records provided by Company B to the FBI, on the same date Employee B responded to the email from Subject Account 2, exchanged several messages, and ultimately sent approximately 3,000 W-2 forms for Company B's employees. According to Company B, Subject Account 2 was not authorized to request or receive this information.

15. Additionally, according to email records provided by Company B to the FBI, on the same date Employee B responded to the email from Subject Account 2, Employee B received another email from Subject Account 2 asking for the "login details to all employee's [sic] payroll." According to the header information for the message, this email address was sent from Subject Account 2 using IP address 154.113.89.134 ("Subject IP Address 3"), which resolves to Nigeria.

***Prior Federal Search Warrant Results for Subject Account 2***

16. On or about March 30, 2018, the Honorable Daniel G. Martin, United States Magistrate Judge for the Northern District of Illinois, issued a search warrant (18 M 217) for Subject Account 2. The FBI received the search warrant results from

Comcast, which I have reviewed. In Subject Account 2, I found material relating to the **Subject Offenses**, including:

a. The February 16, 2018 email (discussed above) from Subject Account 2 to Employee B which stated, "Kindly send me the individual 2017 W-2 (PDF) of our company staff for a quick review," and the response email from Employee B, which contained W-2 forms for approximately 3,000 Company B employees.

b. A February 16, 2018 email from Subject Account 2 sent to Employee C of Company C, which stated, "Kindly send me the individual 2017 W-2 (PDF) of our company staff for a quick review," and a response email from Employee C, which contained W-2 forms for approximately 1,100 Company C employees.

c. A February 16, 2018 email from Subject Account 2 sent to Employee D of Company D, which stated, "Kindly send me the individual 2017 W-2 (PDF) of our company staff for a quick review," and a response email from Employee D, which contained W-2 forms for approximately 300 Company D employees.

d. Approximately 100 additional emails sent from Subject Account 2 between on or about February 15, 2018, and on or about February 16, 2018, each of which stated, "Kindly send me the individual 2017 W-2 (PDF) of our company staff for a quick review." Approximately 100 different organizations were the recipients of these emails, each of which listed a different purported sender's name.

***Comcast Subscriber Records Link Subject Account 2 with Subject Account 7***

17. According to subscriber records received from Comcast, ceo_portals@comcast.net (Subject Account 7), is a deleted user ID that is part of the same Comcast customer account (number ending in 9090) as Subject Account 2.

18. Based on my training and experience, and the context of this case, I believe that an individual or individuals involved in spearphishing may have compromised the legitimate Comcast customer's account (ending in 9090) and used it to create additional email addresses (including Subject Accounts 2 and 7), from which the individual or individuals furthered the fraud scheme.

***Subject Account 7 Requests Fraudulent Wire Transfers from Company E***

19. On or about May 25, 2018, the Honorable Young B. Kim, United States Magistrate Judge for the Northern District of Illinois, issued a search warrant for Subject Account 7 and another account that was part of the fraud scheme. I have reviewed the search warrant results for Subject Account 7.

20. Among the emails seized from Subject Account 7 pursuant to the search warrant, I observed numerous phishing emails which requested fraudulent wire transfers from numerous companies. These emails used the names of legitimate high-ranking employees (although in reality they originated from Subject Account 7), and had subject lines indicative of high urgency.

21. More specifically, on February 23, 2018, Subject Account 7 emailed Employee E of Company E asking if the employee was "available in the office," using the subject "Urgent." The email originated from Subject Account 7, but used the sender name of Company E's Chief Financial Officer. After Employee E responded that he/she was available, Subject Account 7 requested a wire transfer of $46,800 be sent to a Bank of America bank account, and provided the account details. Employee E complied and sent $46,800 to Bank of America account number 237037874904 in the name of Wilanna Gregory. According to Company E, the CFO did not send this email, and the transfer was not authorized.

22. According to an IRS-CI interview with a Bank of America employee, bank account number 237037874904 was opened online on January 16, 2018. On February 28, 2018, Wilanna Gregory came into a Bank of America branch seeking to withdraw funds from the account. Because Gregory did not have a signature card on file, she had to show her North Carolina driver's license, as part of Bank of America's account verification process. During this meeting, the Bank of America employee questioned Gregory regarding the large amount of funds that was wired into her newly opened account. These funds were wired into her account on February 23, 2018 from Company E in the amount of $46,800. According to the bank employee's notes, when asked about the source of these funds in a newly opened account, Gregory stated that she was employed as a nurse, and she "got a loan to pay off debts."

23. Four days later, on or about February 27, 2018, Bank of America records show a cash withdrawal from account number 237037874904. Surveillance video from the branch shows Wilanna Gregory receiving a large quantity of cash from the teller.

24. On or about July 31, 2018 IRS-CI agents interviewed Wilanna Gregory. When initially asked about the Bank of America account, Gregory stated that she did not have any bank accounts. After being shown a signature card for bank account number 237037874904 with her signature, Gregory again denied controlling that account. However, after being shown the surveillance video photograph above of Gregory at the branch, Gregory admitted her involvement. In summary, Gregory stated that she started communicating with someone named "George Pegan" (phonetic spelling) on Facebook in approximately 2017. Gregory used the Facebook name "Beth E Kivett." She stated that Pegan used the Facebook name "George Pegan." According to Gregory, as her relationship with Pegan progressed, she began texting with Pegan in approximately October 2017. Pegan told Gregory that he was employed as a chef in Ohio, but that his company moved him to Nigeria to open a restaurant. Pegan was unable to open a bank account on his own, and needed Gregory to open a bank account so Pegan had somewhere to send a loan he received. According to Gregory, Pegan then opened the account online in Gregory's name, and told Gregory that a wire would be coming into the account. Pegan instructed Gregory to keep $1,200 for herself and wire the rest through Western Union and MoneyGram to

Pegan's friend "Nicholas Edbomyia Jr." in Nigeria. Gregory then admitted to withdrawing the funds from Bank of America at Pegan's request, and to wiring the money as instructed.

***Subject Account 18 Attempts to Spearphish Company E***

25. Subsequent phishing emails involving fraudulent wire requests were sent to Company E from multiple email accounts not associated with Company E between February 2018 and April 2018.

26. Most recently, **Subject Account 18**, using the Chief Executive Officer of Company E's name, emailed Employee E asking, "Are you in the office?" with a subject line "Urgent Request." This email has several characteristics that closely resemble the spearphishing emails sent from Subject Account 7 to Company E earlier in 2018, including:

a. The message was sent to the same employee, namely Employee E;

b. The message appeared to originate from Company E's CFO; and

c. The subject line and body of the email are nearly identical to the prior spearphishing attempt.

27. Based on my training and experience, conversations with other experienced agents, and the context of this case, I believe that there is a fair probability that the user of **Subject Account 18** was attempting to spearphish Company E by requesting an additional fraudulent wire transfer.

***Training and Experience***

28. Based on my training and experience in computer-related investigations, and based on conversations with other experienced agents, I believe that a search of email contained in the **Subject Account 18** will likely yield investigative leads relating to:

a. the identity of the individual(s) and co-conspirators involved in the spear-phishing attacks against multiple victim companies;

b. the identity, location, and contact information of the account user(s) and possible co-conspirators involved in the scheme;

c. communications among co-conspirators and other individuals involved in the scheme;

d. the identification of additional communication accounts utilized by the account user(s); and

e. the methods, techniques, and tools used to conduct the illegal activities.

29. Regarding searches of Google accounts in particular, based on my training and experience, and conversations with other experienced agents, I have learned that:

a. Individuals involved in computer crimes, such as phishing, may use Google searches to learn information about the targets of the emails, as well as background information used in creating the fictitious emails (e.g., information about

the purported sender, or the content of the message). Additionally, Google searches for non-criminal topics (e.g., driving directions or searches for locations in one's neighborhood) can reveal information about the identity of the user of the account. As a result, a warrant for Google search history can provide valuable investigative information about the identity of the person who drafted or sent the phishing email.

b. Search warrants for location information stored by Google (including Google Maps), when viewed in combination with email content, can help to identify the user of the account by correlating the messages with the user's location at specific times. For example, location information can show the locations the user frequented (e.g., home, work, school) at certain times, which can help differentiate that person from other individuals, even those who might live in the same home or work at the same office.

c. Individuals may store large quantities of files in Google Drive, including files that they send or receive through Gmail. Additionally, if an individual views attachments to Gmail messages through certain Google apps, Google may retain the file itself in Google Drive. Google Drive also allows users to collaborate with others in creating, editing, or sharing files. As such, it can produce investigative leads concerning co-conspirators, or others who may be aware of the activities of the account's user.

## III. SEARCH PROCEDURE

30. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Google to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Google personnel who will be directed to the information described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, Google employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact duplicate of all information stored in the computer accounts and files described therein;

31. Google employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

32. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records received from Google employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

## IV. CONCLUSION

33. Based on the above information, I respectfully submit that there is probable cause to believe that evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 1028, 1028A, and 1343 are located within one or more computers and/or servers found at Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. By this affidavit and application, I request that the Court issue a search warrant directed to Google allowing agents to seize the electronic evidence and other information stored on the Google servers following the search procedure described in Attachment A and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.

Timothy J. Malak
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 26th day of October, 2018

Honorable SUSAN E. COX
United States Magistrate Judge

# ATTACHMENT A

## I. SEARCH PROCEDURE

1. The search warrant will be presented to Google personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Google employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant. Google shall disclose responsive data, if any, by sending to FBI Special Agent Timothy J. Malak, Federal Bureau of Investigation, 2111 W. Roosevelt Road, Chicago, Illinois 60608.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

## II. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES OF GOOGLE

To the extent that the information described below in Section III is within the possession, custody, or control of Google, which are stored at premises owned,

maintained, controlled, or operated by Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, Google is required to disclose the following information to the government for the following account, regardless of whether such information is stored, held or maintained inside or outside of the United States:

**Executivedata58@gmail.com**

a. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.

b. All electronic files stored online via Google Drive, stored and presently contained in, or on behalf of the account described above.

c. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.

d. All existing printouts from original storage of all the electronic mail described above.

e. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.

f. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing and payment records.

g. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.

h. All account contents previously preserved by Google, in electronic or printed form.

i. All subscriber records for any Google account associated by cookies, recovery email address, or telephone number to the account described above.

j. All Google Map data, including geo-location history, location search history and associated timestamps.

k. Business records listing all the Google products utilized by each of the Google accounts described above.

## III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence, instrumentalities, and fruits concerning violations of Title 18, United States Code, Sections 1028, 1028A, and 1343, as follows:

Electronic files, including computer source code, computer executable programs, email messages, electronic communications, attachments, and any other electronic files that contain information regarding:

1. The identity of the user(s) of the Subject Accounts, including location information identifying the user(s)

2. Information relating to proceeds from criminal activity

3. Company B, Employee B, and Individual B

4. Company C and Employee C

5. Company D and Employee D

6. Company E and Employee E

7. W-2 or other tax forms

8. Social security numbers

9. Identities of victims of identity theft

10. Phishing or spear-phishing

11. Identity theft

12. Banking information relating to the **Subject Offenses**

13. Money or wire transfer services relating to the **Subject Offenses**

14. Wilanna Gregory

15. George Pegan

16. The identity and location of person(s) who communicated with the account user(s) relating to the crime under investigation

17. Items relating to the identities or locations of the users of the Google accounts or other participants of the scheme; and

18. All of the non-content records and information described in Section II.

## ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the free web-based electronic mail service provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.

b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.

c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or

d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such

electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

AO 93 (Rev. 11/13) Search and Seizure Warrant AUSA Sean K. Driscoll, (312) 469-6151

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

**UNDER SEAL**

In the Matter of the Search of:

The Google account executivedata58@gmail.com, further described in Attachment A

Case Number: 18M678

# SEARCH AND SEIZURE WARRANT

To: Timothy J. Malak and any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California:

**See Attachment A**

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

**See Attachment A**

**YOU ARE HEREBY COMMANDED** to execute this warrant on or before November 9, 2018 in the daytime (6:00 a.m. to 10:00 p.m.).

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the issuing United States Magistrate Judge.

Date and time issued: October 26, 2018 @ 11:20 AM

*Judge's signature*

City and State: Chicago, Illinois

SUSAN E. COX, U.S. Magistrate Judge
*Printed name and title*

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

## Return

| Case No: | Date and Time Warrant Executed: | Copy of Warrant and Inventory Left With: |
|---|---|---|
| | | |

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
*Executing officer's signature*

_____
*Printed name and title*

# ATTACHMENT A

## I. SEARCH PROCEDURE

1. The search warrant will be presented to Google personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Google employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant. Google shall disclose responsive data, if any, by sending to FBI Special Agent Timothy J. Malak, Federal Bureau of Investigation, 2111 W. Roosevelt Road, Chicago, Illinois 60608.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

## II. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES OF GOOGLE

To the extent that the information described below in Section III is within the possession, custody, or control of Google, which are stored at premises owned,

maintained, controlled, or operated by Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, Google is required to disclose the following information to the government for the following account, regardless of whether such information is stored, held or maintained inside or outside of the United States:

**Executivedata58@gmail.com**

a. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.

b. All electronic files stored online via Google Drive, stored and presently contained in, or on behalf of the account described above.

c. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.

d. All existing printouts from original storage of all the electronic mail described above.

e. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.

f. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing and payment records.

g. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.

h. All account contents previously preserved by Google, in electronic or printed form.

i. All subscriber records for any Google account associated by cookies, recovery email address, or telephone number to the account described above.

j. All Google Map data, including geo-location history, location search history and associated timestamps.

k. Business records listing all the Google products utilized by each of the Google accounts described above.

## III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence, instrumentalities, and fruits concerning violations of Title 18, United States Code, Sections 1028, 1028A, and 1343, as follows:

Electronic files, including computer source code, computer executable programs, email messages, electronic communications, attachments, and any other electronic files that contain information regarding:

1. The identity of the user(s) of the Subject Accounts, including location information identifying the user(s)

2. Information relating to proceeds from criminal activity

3. Company B, Employee B, and Individual B

4. Company C and Employee C

5. Company D and Employee D

6. Company E and Employee E

7. W-2 or other tax forms

8. Social security numbers

9. Identities of victims of identity theft

10. Phishing or spear-phishing

11. Identity theft

12. Banking information relating to the **Subject Offenses**

13. Money or wire transfer services relating to the **Subject Offenses**

14. Wilanna Gregory

15. George Pegan

16. The identity and location of person(s) who communicated with the account user(s) relating to the crime under investigation

17. Items relating to the identities or locations of the users of the Google accounts or other participants of the scheme; and

18. All of the non-content records and information described in Section II.

## ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the free web-based electronic mail service provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.

b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.

c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or

d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such

electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.